Граница свободного расстояния случайных кодов с (частично) единичной памятью

Кондрашов К.А.
Институт проблем передачи информации им. А.А. Харкевича РАН
k_kondrashov@iitp.ru

Зяблов В.В.
Институт проблем передачи информации им. А.А. Харкевича РАН
zyablov@iitp.ru

Аннотация

Рассмотрены двоичные сверточные коды с (частично) единичной памятью на основе случайных блоковых кодов. Получена нижняя граница свободного расстояния случайных кодов с (частично) единичной памятью.

1. Введение

Коды с *единичной памятью* (ЕП) были предложены Ли [1] в 1976 году. ЕП–коды относятся к специальному классу сверточных (b,c,m) – кодов. ЕП–коды — это сверточные коды со скоростью b/c, памятью $m=1$ и длиной суммарного кодового ограничения $\nu = b$. В [2], Лауэр развил идею кодов с единичной памятью и представил коды с *частично единичной памятью* (ЧЕП). Как и коды с единичной памятью, они обладают памятью $m=1$, но длина их суммарного кодового ограничения меньше: $\nu < b$. ЕП–коды строятся на основе блоковых кодов, например, кодов *Рида–Соломона* [3] или кодов БЧХ [4, 5], что упрощает их исследование. Оно фактически сводится к анализу блоковых кодов, лежащих в основе.

Простые верхние границы свободного расстояния ЕП–кодов на основе границ сверточных кодов были даны в [1], [2]. Однако в работе [6] К. Томмесен и Й. Юстесен установили отличие в корректирующих свойствах ЕП–кодов и сверточных кодов с произвольно большой памятью. Было показано, что ЕП–коды могут обладать превосходящими характеристиками по сравнению со сверточными кодами с произвольной памятью.

В данной работе рассматривается ансамбль (Ч)ЕП–кодов, построенных на основе блоковых кодов со случайными проверочными матрицами. Для заданного ансамбля кодов выводится нижняя граница свободного расстояния.

2. Базовые определения

Пусть информационная последовательность состоит из блоков $\mathbf{u}_t = (u_{t1}, u_{t2}, \ldots, u_{tb})$, $t = 0,1,\ldots$, где u_{ti}, $i = 1..b$ – двоичные символы. Тогда кодовая последовательность (b,c)–ЕП кода, состоящая из блоков $\mathbf{v}_t = (v_{t1}, v_{t2}, \ldots, v_{tc})$, получается по следующему правилу:

$$\mathbf{v}_t = \mathbf{u}_t \mathbf{G}_0(t) + \mathbf{u}_{t-1}\mathbf{G}_1(t), \qquad (1)$$

где матрицы $\mathbf{G}_0(t)$, $\mathbf{G}_1(g)$ имеют размер $b \times c$. Матрица $\mathbf{G}_0(t)$ имеет полный ранг: $\mathrm{rk}\mathbf{G}_0(t) = b$. Ранг $G_1(t)$ определяет, имеет ли код полную или частичную единичную память. Если матрицы $\mathbf{G}_0$, $\mathbf{G}_1$ не зависят от t, то код называется постоянным. В противном случае код является переменным во времени. Переменный код будем называть периодическим, с периодом T, если выполняется

$$\mathbf{G}_i(t+T) = \mathbf{G}_i(t),\ i = 0,1;\ t = 0,1\ldots$$

Порождающее уравнение (1) можно переписать в виде $\mathbf{v} = \mathbf{uG}$, где $\mathbf{G}$ – полубесконечная порождающая матрица:

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0(0) & \mathbf{G}_1(1) & \mathbf{0} & \mathbf{0} & \cdots \\ \mathbf{0} & \mathbf{G}_0(1) & \mathbf{G}_1(2) & \mathbf{0} & \cdots \\ \mathbf{0} & \mathbf{0} & \mathbf{G}_0(2) & \mathbf{G}_1(3) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{bmatrix}. \qquad (2)$$

Важной характеристикой сверточного кода, определяющей его корректирующие свойства, является *свободное расстояние* d_{free}. Свободное расстояние d_{free} – это минимальное хэммингово расстояние между двумя различными кодовыми

последовательностями. Для его определения обычно вводится дополнительная характеристика – *активное строчное расстояние* $\hat{d}_n^r$. Активное строчное расстояние $\hat{d}_n^r$ показывает минимальное расстояние между различными кодовыми словами, соответствующими путям на минимальной кодовой решетке, выходящим из нулевого состояния на некоторой глубине t и возвращающимся в нулевое состояние в первый раз на глубине $t+n+1$. Обозначим с помощью $I_{t,n}$ множество всех информационных последовательностей $\mathbf{u}$, таких что $\mathbf{u}_{t+i} \neq \mathbf{0}$ при $i = 0,\ 1,\ \ldots, n$ и $\mathbf{u}_i = \mathbf{0}$ при $i < t$ и $i > t+n$. Тогда $\hat{d}_n^r$ можно записать как

$$\hat{d}_n^r = \min_t \min_{\mathbf{u}\in I_{t,n}} \{\omega_H(\mathbf{uG})\}, \qquad (3)$$

Свободное расстояние связано с активными строчными расстояниями следующим соотношением:

$$d_{free} = \min_{n=1,2,\ldots} \{\hat{d}_n^r\}. \qquad (4)$$

3. Ансамбль случайных (Ч)ЕП–кодов

Линейный код может быть задан как порождающей, так и проверочной матрицей. Введем ансамбль двоичных $\mathscr{E}(b,c,\nu)$–(Ч)ЕП кодов с полубесконечной проверочной матрицей вида:

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_0(0) & \mathbf{0} & \mathbf{0} & \cdots \\ \mathbf{H}_1(1) & \mathbf{H}_0(1) & \mathbf{0} & \cdots \\ \mathbf{0} & \mathbf{H}_1(2) & \mathbf{H}_0(2) & \cdots \\ \mathbf{0} & \mathbf{0} & \mathbf{H}_1(3) & \cdots \\ \vdots & \vdots & \vdots & \end{bmatrix}. \qquad (5)$$

Матрицы $\mathbf{H}_i(t)$ имеют размер $(r \times c)$, где $r = c - b$. Двоичные элементы компонентных матриц выбираются случайно равновероятно. Матрицы $\mathbf{H}_0(t)$ имеют полный ранг $\mathrm{rk}\mathbf{H}_0(t) = r$, в то время как матрицы $\mathbf{H}_1(t)$ могут иметь меньший ранг. Ансамбль $\mathscr{E}$ состоит из кодов с проверочными матрицами вида (5) такими, что соответствующие им порождающие матрицы имеют вид (2). Если порождающая и проверочная матрицы сверточного кода заданы в минимальной базовой кодирующей форме, то их суммарные кодовые ограничения должны совпадать [7]. Таким образом:

$$\nu = \mathrm{rk}(\mathbf{G}_1(t)) = \mathrm{rk}(\mathbf{H}_1(t)). \qquad (6)$$

Ограничение (6) позволяет определить ансамбль $\mathscr{E}(b,c,\nu)$ таким, что при скоростях $R < 0.5$ коды из $\mathscr{E}$ имеют полную единичную память, а при скоростях $R \geq 0.5$ – частично единичную. При частичной памяти ранг $\mathrm{rk}(\mathbf{G}_1) = b_1$, $b_1 < b$. Без потери общности можно считать, что

$$\mathbf{G}_0(t) = \begin{bmatrix} \mathbf{G}_{00}(t) \\ \mathbf{G}_{01}(t) \end{bmatrix}, \quad \mathbf{G}_1(t) = \begin{bmatrix} \mathbf{0} \\ \mathbf{G}_{11}(t) \end{bmatrix}, \qquad (7)$$

где подматрицы $\mathbf{G}_{00}(t)$ и $\mathbf{G}_{01}(t)$, $\mathbf{G}_{11}(t)$ имеют размеры $(b - b_1 \times c)$ и $(b_1 \times c)$, соответственно. В данной работе рассматривается ансамбль $\mathscr{E}(b,c,\nu = b_1)$, удовлетворяющий условию

$$\mathrm{rk}\begin{bmatrix} \mathbf{G}_{11}(t) \\ \mathbf{G}_{00}(t) \\ \mathbf{G}_{01}(t) \end{bmatrix} = b + b_1 < c. \qquad (8)$$

Условие (8) потребуется в дальнейшем при анализе активных строковых и свободного расстояния.

Теорема 1. Для любой полубесконечной матрицы $\mathbf{H}$ с подматрицами $\mathbf{H}_0(t)$, имеющими размер $(r \times c)$ и полный ранг $\mathrm{rk}\mathbf{H}_0(t) = r$, и подматрицами $\mathbf{H}_1(t)$ с тем же размером и рангом $\mathrm{rk}\mathbf{H}_1(t) = \alpha r$, $\alpha = \alpha(R)$, $0 < \alpha \leq 1$ существует порождающая матрица $\mathbf{G}$ такая, что $\mathbf{GH}^{\mathrm{T}} = \mathbf{0}$ и матрица $\mathbf{G}$ задает $\mathscr{E}(b = Rc, c, \nu = \alpha r)$ –(Ч)ЕП код.

Доказательство. Порождающая матрица $\mathbf{G}$ (Ч)ЕП–кода состоит из двух подматриц: $\mathbf{G}_0$ и $\mathbf{G}_1$. Покажем, что эти матрицы содержат больше неизвестных, чем есть уравнений, которым они должны удовлетворять, и, следовательно, матрица $\mathbf{G}$ всегда существует. Условию $\mathbf{G}\cdot\mathbf{H}^{\mathrm{T}} = \mathbf{0}$ соответствуют следующие уравнения:

$$\begin{aligned} &\mathbf{G}_0(t)\cdot\mathbf{H}_0^{\mathrm{T}}(t-1) = \mathbf{0}, \\ &\mathbf{G}_0(t)\cdot\mathbf{H}_1^{\mathrm{T}}(t) + \mathbf{G}_1(t+1)\cdot\mathbf{H}_0^{\mathrm{T}}(t) = \mathbf{0}, \\ &\mathbf{G}_1(t+1)\cdot\mathbf{H}_1^{\mathrm{T}}(t+1) = \mathbf{0}. \end{aligned}$$

Среди них возможно не более $2br + \nu^2$ линейно независимых уравнений. Дополнительно, мы должны гарантировать, что $\mathrm{rk}(\mathbf{G}_0) = b$. Этого всегда можно добиться, выбрав случайную $b \times b$ подматрицу в матрице $\mathbf{G}_0$ и положив ее нижне– или верхнетреугольной. Иными словами, нужно разместить $\sum_{i=1}^{b-1} i = b(b-1)/2$ нулевых элементов в определенных позициях матрицы $\mathbf{G}_0$. Следовательно, добавляется еще $b(b-1)/2$ уравнений. Всего в матрице $\mathbf{G}$ неизвестных элементов $(b+\nu)c$. Следовательно, число свободно выбираемых переменных g_{free} удовлетворяет неравенству:

$$\begin{aligned} g_{free} &\geq (b+\nu)c - 2br - \nu^2 - (b(b-1))/2 \\ &> bc + \nu c - 2b(1-R)c - \nu^2 - b^2/2 \\ &= \nu c - \nu^2 - Rc^2 + \tfrac{3}{2}R^2c^2. \end{aligned}$$

Квадратное уравнение относительно ν

$$\nu^2 - \nu c + Rc^2 - \frac{3}{2}R^2c^2 = 0 \qquad (9)$$

имеет вещественные корни при любой скорости R. Более того, при любой $\nu = \alpha r = \mathrm{rk}(G_1) \leq b$ выполняется

$$\nu^2 - \nu c + Rc^2 - \frac{3}{2}R^2c^2 \leq 0. \qquad (10)$$

Следовательно, $g_{free} \geq 0$ и теорема доказана. □

4. Нижняя граница свободного расстояния

Для получения нижней границы свободного расстояния (Ч)ЕП–кодов из ансамбля $\mathscr{E}(b,c,\nu)$ исследуем их активные строчные расстояния. Рассмотрим все кодовые последовательности, порожденные информационными последовательностями различной длины n, начинающимися и заканчивающимися нулевой серией и не содержащими нулевых блоков внутри: $\mathbf{u} \in I_{t,n}$. Для простоты будем считать коды постоянными во времени. Полученные результаты, если не оговорено отдельно, будут верны и для периодических кодов.

Проведем анализ кодовых последовательностей $\mathscr{E}(b,c,b_1)$–кодов с частично единичной памятью. Пусть матрицы $\mathbf{G}_0$, $\mathbf{G}_1$ представлены в виде (7), $\mathrm{rk}(\mathbf{G}_1) = b_1 < b$. Разобьем информационные блоки на две части из $b - b_1$ и b_1 двоичных символов, соответственно: $\mathbf{u}_t = (\mathbf{u}_{t,0}\ \mathbf{u}_{t,1})$. В соответствии с кодирующим правилом,

$$\mathbf{v} = \begin{bmatrix} \vdots \\ \mathbf{u}_{t,0}^{\mathrm{T}} \\ \mathbf{u}_{t,1}^{\mathrm{T}} \\ \mathbf{u}_{t+1,0}^{\mathrm{T}} \\ \mathbf{u}_{t+1,1}^{\mathrm{T}} \\ \vdots \end{bmatrix}^{\mathrm{T}} \cdot \begin{pmatrix} \ddots & & & & & \\ \mathbf{G}_{00} & \mathbf{0} & & & & \\ \mathbf{G}_{01} & \mathbf{G}_{11} & & & & \\ & \mathbf{G}_{00} & \mathbf{0} & & & \\ & \mathbf{G}_{01} & \mathbf{G}_{11} & & & \\ & & & \mathbf{G}_{00} & \mathbf{0} & \\ & & & \mathbf{G}_{01} & \mathbf{G}_{11} & \\ & & & & & \ddots \end{pmatrix}. \quad (11)$$

Исследуем результаты произведения (11) при $n = 1, 2, \ldots$.

A. $n = 1$

Пусть $\mathbf{u} = [\ldots, \mathbf{0}, \mathbf{u}_t, \mathbf{0}, \ldots]$, где $\mathbf{u}_t = (\mathbf{u}_{t,0}\ \mathbf{u}_{t,1})$, $\mathbf{u}_t \neq \mathbf{0}$. Распишем результаты произведения (11):

$$\begin{aligned} \mathbf{v} &= [\ldots, \mathbf{0}, \mathbf{v}_t, \mathbf{v}_{t+1}, \mathbf{0}, \ldots], \\ \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11}. \end{aligned}$$

Для случайного ненулевого информационного блока $\mathbf{u}_t = (\mathbf{u}_{t,0}\ \mathbf{u}_{t,1})$ возможны 3 случая.

1. На входе:
$$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} = \mathbf{0}.$$
На выходе:
$$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00}, \\ \mathbf{v}_{t+1} &= \mathbf{0}. \end{aligned}$$
Обозначим с помощью C_{00} код, заданный порождающей матрицей $\mathbf{G}_{00}$. Тогда $\mathbf{v}_t \in C_{00}$ и хэммингов вес кодовой последовательности $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}) \geq d(C_{00})$, где $d(C_{00})$ – кодовое расстояние блокового кода C_{00}.

2. На входе:
$$\mathbf{u}_{i,0} \neq \mathbf{0},\ \mathbf{u}_{i,1} \neq \mathbf{0}.$$
На выходе:
$$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11}. \end{aligned}$$
Пусть C_0 означает код, заданный порождающей матрицей $\mathbf{G}_0$, а C_{11} – порождающей матрицей $\mathbf{G}_{11}$. Тогда $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{11}$ и вес кодовой последовательности $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}) \geq d(C_0) + d(C_{11})$.

3. На входе:
$$\mathbf{u}_{i,0} = \mathbf{0},\ \mathbf{u}_{i,1} \neq \mathbf{0}.$$
На выходе:
$$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11}. \end{aligned}$$
Обозначим с помощью C_{01} код, заданный порождающей матрицей $\mathbf{G}_{01}$. Тогда $\mathbf{v}_t \in C_{01}$, $\mathbf{v}_{t+1} \in C_{11}$ и $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}) \geq d(C_{01}) + d(C_{11})$.

Активное расстояние d_1^r соответствует минимальному весу рассмотренных выше кодовых последовательностей. Пусть при равной длине кодов, коды с меньшей скоростью имеют большее кодовое расстояние. Случайные блоковые коды лежат на границе Варшамова–Гилберта [?] и для них данное предположение выполняется. Тогда $d(C_0) < d(C_{01})$ и минимальный возможный вес в случае 2 меньше, чем в случае 3. Сравним случаи 1 и 2. Кодовое расстояние $d(C_{00})$ больше $d(C_0)$. Однако $d(C_{00})$ может быть меньше суммы $d(C_0) + d(C_{11})$. Последняя определяется отношением между b и b_1. Так, если $b - b_1 > b_1$, то $d(C_{00}) < d(C_{11})$ и $d_1^r = d(C_{00})$. Таким образом, $\hat{d}_1^r = \min(d(C_{00}), d(C_0) + d(C_{11}))$.

B. $n = 2$

Пусть информационная последовательность $\mathbf{u}$ состоит из 2 последовательных ненулевых блоков $\mathbf{u} = [\ldots, \mathbf{0}, \mathbf{u}_t, \mathbf{u}_{t+1}, \mathbf{0}, \ldots]$, где $\mathbf{u}_i = (\mathbf{u}_{i,0}\ \mathbf{u}_{i,1})$, $i = t, t+1$. Исследуем все возможные кодовые последовательности, порождаемые информационной последовательностью такого вида. Из уравнения (11):

$$\begin{aligned} \mathbf{v} &= [\ldots, \mathbf{0}, \mathbf{v}_t, \mathbf{v}_{t+1}, \mathbf{v}_{t+2}, \mathbf{0}, \ldots], \\ \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11} + \mathbf{u}_{t+1,0}\mathbf{G}_{00} + \mathbf{u}_{t+1,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_{11}. \end{aligned}$$

Рассмотрим возможные случаи.

1. На входе:

   $\mathbf{u}_{t,0} \neq \mathbf{0}$, $\mathbf{u}_{t,1} = \mathbf{0}$, блок $\mathbf{u}_{t+1}$произвольный ненулевой.

   На выходе:

   $$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t+1,0}\mathbf{G}_{00} + \mathbf{u}_{t+1,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_{11}. \end{aligned}$$

   Получаем, $\mathbf{v}_t \in C_{00}$, а блоки $\mathbf{v}_{t+1}$, $\mathbf{v}_{t+2}$ соответствуют кодовым блокам, рассмотренным в случае $n = 1$. Таким образом, $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}) \geq d(C_{00}) + \hat{d}_1^r$.

2. На входе:

   $$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \mathbf{u}_{t+1,0} \neq \mathbf{0},\ \mathbf{u}_{t+1,1} = \mathbf{0}.$$

   На выходе:

   $$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11} + \mathbf{u}_{t+1,0}\mathbf{G}_{00}, \\ \mathbf{v}_{t+2} &= \mathbf{0}. \end{aligned}$$

   Если матрица

   $$\mathbf{G}_{m0} = \begin{pmatrix} \mathbf{G}_{11} \\ \mathbf{G}_{00} \end{pmatrix}$$

   задает код C_{m0}, то $\mathbf{v}_{i+1} \neq \mathbf{0}$, так как порождающий его информационный блок ненулевой: $\mathbf{u}_{t,1} \neq \mathbf{0}$, $\mathbf{u}_{t+1,0} \neq \mathbf{0}$. Получаем, $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{m0}$ и $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{0}) \geq d(C_0) + d(C_{m0})$.

3. На входе:

   $$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \mathbf{u}_{t+1,0} = \mathbf{0},\ \mathbf{u}_{t+1,1} \neq \mathbf{0}$$

   На выходе:

   $$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11} + \mathbf{u}_{t+1,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_{11}. \end{aligned}$$

   Если матрица

   $$\mathbf{G}_{m1} = \begin{pmatrix} \mathbf{G}_{11} \\ \mathbf{G}_{01} \end{pmatrix}$$

   задает код C_{m1}, то $\mathbf{v}_{i+1} \neq \mathbf{0}$. Получаем, $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{m1}$, $\mathbf{v}_{t+2} \in C_{11}$ и $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}) \geq d(C_0) + d(C_{m1}) + d(C_{11})$.

4. На входе:

   $$\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \mathbf{u}_{t+1,0} \neq \mathbf{0},\ \mathbf{u}_{t+1,1} \neq \mathbf{0}.$$

   На выходе:

   $$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11} + \mathbf{u}_{t+1,0}\mathbf{G}_{00} + \mathbf{u}_{t+1,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_{11}. \end{aligned}$$

   Если матрица

   $$\mathbf{G}_p = \begin{pmatrix} \mathbf{G}_{11} \\ \mathbf{G}_{00} \\ \mathbf{G}_{01} \end{pmatrix}$$

   задает код C_p, то $\mathbf{v}_{i+1} \neq \mathbf{0}$. Получаем, $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_p$, $\mathbf{v}_{t+2} \in C_{11}$ Вес кодовой последовательности $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}) \geq d(C_0) + d(C_p) + d(C_{11})$.

5. На входе:

   $$\mathbf{u}_{t,0} = \mathbf{0},\ \mathbf{u}_{t,1} \neq \mathbf{0},\ \text{ненулевой } \mathbf{u}_{t+1}.$$

   В зависимости от $\mathbf{u}_{i+1}$, этот случай будет покрываться случаями 2–4 с тем исключением, что $\mathbf{v}_t \notin C_0$, $\mathbf{v}_t \in C_{01}$. Так как $d(C_{01}) > d(C_0)$, то вес получившейся последовательности будет всегда больше, чем в случаях 2–4.

Определим минимальный вес среди возможных случаев. Сравним случаи 3 и 4:

$$d(C_0) + d(C_{m1}) + d(C_{11}) > d(C_0) + d(C_p) + d(C_{11}),$$

так как $d(C_{m1}) > d(C_p)$: $\dim(G_{m1}) = 2b_1$, $\dim(G_\alpha) = b + b_1$, а $2b_1 < b + b_1$.
Сравним случаи 4 и 2:

$$d(C_0) + d(C_p) + d(C_{11}) > d(C_0) + d(C_{m0}),$$

так как $d(C_{11}) > d(C_{m0})$: $\dim(G_{11}) = b_1$, $\dim(G_{m0}) = b$, а $b_1 < b$.
Сравним случаи 1 и 2:

$$d(C_{00}) + \min(d(C_{00}),\ d(C_0) + d(C_{11})) > d(C_0) + d(C_{m0}),$$

так как $d(C_{00}) > d(C_{m0})$, $d(C_{00}) > d(C_0)$, а $\min(d(C_{00}),\ d(C_0) + d(C_{11}))$ больше $d(C_0)$ в любом случае. Таким образом, $\hat{d}_2^r = d(C_0) + d(C_{m0})$.

C. $n = 3$

Пусть информационная последовательность $\mathbf{u}$ состоит из 2 последовательных ненулевых блоков $\mathbf{u} = [\ldots, \mathbf{0}, \mathbf{u}_t, \mathbf{u}_{t+1}, \mathbf{u}_{t+2}, \mathbf{0}, \ldots]$, где $\mathbf{u}_i = (\mathbf{u}_{i,0}\ \mathbf{u}_{i,1})$, $i = t, t+1, t+2$. Исследуем все возможные кодовые последовательности, порождаемые информационной последовательностью такого вида. Из уравнения (11):

$$\begin{aligned} \mathbf{v} &= [\ldots, \mathbf{0}, \mathbf{v}_t, \mathbf{v}_{t+1}, \mathbf{v}_{t+2}, \mathbf{v}_{t+3}, \mathbf{0}, \ldots], \\ \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11} + \mathbf{u}_{t+1,0}\mathbf{G}_{00} + \mathbf{u}_{t+1,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_{11} + \mathbf{u}_{t+2,0}\mathbf{G}_{00} + \mathbf{u}_{t+2,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+3} &= \mathbf{u}_{t+2,1}\mathbf{G}_{11}. \end{aligned}$$

Рассмотрим основные случаи.

1. На входе:

   $\mathbf{u}_{t,0} \neq \mathbf{0},\ \mathbf{u}_{t,1} = \mathbf{0},$ произвольные $\mathbf{u}_{t+1}, \mathbf{u}_{t+2}$.

   На выходе:

$$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{i,0}\mathbf{G}_{00}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t+1,0}\mathbf{G}_{00} + \mathbf{u}_{t+1,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_{11} + \mathbf{u}_{t+2,0}\mathbf{G}_{00} + \mathbf{u}_{t+2,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+3} &= \mathbf{u}_{t+2,1}\mathbf{G}_{11}. \end{aligned}$$

   Блок $\mathbf{v}_t \in C_{00}$. В зависимости от распределения нулевых частей в $\mathbf{u}_{t+1}$ и $\mathbf{u}_{t+2}$ кодовые блоки $\mathbf{v}_{t+1}$, $\mathbf{v}_{t+2}$, $\mathbf{v}_{t+3}$ относятся к кодам и случаям, рассмотренным при изучении $\hat{d}_2^r$. Вес кодовой последовательности $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}\ \mathbf{v}_{t+3}) \geq d(C_{00}) + \hat{d}_2^r$.

2. На входе:

   $\mathbf{u}_{t,0} \neq \mathbf{0}$, $\mathbf{u}_{t,1} \neq \mathbf{0}$, $\mathbf{u}_{t+1,0} \neq \mathbf{0}$, $\mathbf{u}_{t+1,1} = \mathbf{0}$, ненулевой $\mathbf{u}_{t+2}$.

   На выходе:

$$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11} + \mathbf{u}_{t+1,0}\mathbf{G}_{00}, \\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+2,0}\mathbf{G}_{00} + \mathbf{u}_{t+2,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+3} &= \mathbf{u}_{t+2,1}\mathbf{G}_{11}. \end{aligned}$$

   Блоки $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_{m0}$, а блоки $\mathbf{v}_{t+2}$, $\mathbf{v}_{t+3}$ соответствуют случаям, рассмотренным при анализе $\hat{d}_1^r$. Вес последовательности $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}\ \mathbf{v}_{t+3}) \geq d(C_0) + d(C_{m0}) + \hat{d}_1^r$. Далее мы опустим случай отличающийся только тем, что $\mathbf{u}_{t,0} = \mathbf{0}$. Результат будет аналогичным, за исключением $\mathbf{v}_i \in C_{00}$, а это увеличит вес. На входе:

   $\mathbf{u}_{t,0} \neq \mathbf{0}$, $\mathbf{u}_{t,1} \neq \mathbf{0}$, $\mathbf{u}_{t+1,0} \neq \mathbf{0}$, $\mathbf{u}_{t+1,1} \neq \mathbf{0}$, ненулевой $\mathbf{u}_{i+2,0}$.

   На выходе:

$$\begin{aligned} \mathbf{v}_t &= \mathbf{u}_{t,0}\mathbf{G}_{00} + \mathbf{u}_{t,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+1} &= \mathbf{u}_{t,1}\mathbf{G}_{11} + \mathbf{u}_{t+1,0}\mathbf{G}_{00} + \mathbf{u}_{t+1,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+2} &= \mathbf{u}_{t+1,1}\mathbf{G}_{11} + \mathbf{u}_{t+2,0}\mathbf{G}_{00} + \mathbf{u}_{t+2,1}\mathbf{G}_{01}, \\ \mathbf{v}_{t+3} &= \mathbf{u}_{t+2,1}\mathbf{G}_{11}. \end{aligned}$$

   Блоки $\mathbf{v}_t \in C_0$, $\mathbf{v}_{t+1} \in C_p$, а блоки $\mathbf{v}_{t+2}$, $\mathbf{v}_{t+3}$ соответствуют случаям 2–4 анализа $\hat{d}_2^r$. Вес последовательности $\mathrm{wt}(\mathbf{v}_t\ \mathbf{v}_{t+1}\ \mathbf{v}_{t+2}\ \mathbf{v}_{t+3}) \geq d(C_0) + d(C_p) + d(C_{m0})$. Напомним, что $d(C_0) + d(C_{m0}) = \hat{d}_2^r$.

Из рассмотрения опущены случаи, когда $\mathbf{u}_{t,0} = \mathbf{0}$, $\mathbf{u}_{t,1} \neq \mathbf{0}$ или $\mathbf{u}_{t+1,0} = \mathbf{0}$, $\mathbf{u}_{t+1,1} \neq \mathbf{0}$. Они дают результаты, похожие на результаты в случаях 2 или 3, но с большим весом. Определим минимальный вес среди возможных случаев. Сравним случаи 1 и 3:

$$d(C_{00}) + \hat{d}_2^r > d(C_p) + \hat{d}_2^r.$$

Сравним случаи 2 и 3:

$$d(C_0) + d(C_{m0}) + \hat{d}_1^r > d(C_0) + d(C_{m0}) + d(C_p).$$

Получаем, $\hat{d}_3^r = d(C_0) + d(C_{m0}) + d(C_p) = \hat{d}_2^r + d(C_p)$. При дальнейшем анализе видно, что начиная с $n = 2$, активные строчные расстояния растут по закону

$$\hat{d}_n^r \geq \hat{d}_2^r + (n-2)d(C_p). \tag{12}$$

Полученные оценки свободного и активных расстояний верны только в том случае, если матрицы $\mathbf{G}_{m0}$, $\mathbf{G}_{m1}$, $\mathbf{G}_p$ порождают коды и, следовательно, кодовые блоки внутри кодовых последовательностей $\mathbf{uG}$, $\mathbf{u} \in I_{t,n}$ ненулевые.

Лемма 1. При $\mathrm{rk}\mathbf{G}_0 = b$, $\mathrm{rk}\mathbf{G}_1 = b_1$, $b + b_1 < c$ существуют $\mathscr{E}(b, c, b_1)$–(Ч)ЕП коды такие, что $\mathrm{rk}\mathbf{G}_p = b + b_1$, $\mathrm{rk}\mathbf{G}_{m0} = b$, $\mathrm{rk}\mathbf{G}_{m1} = 2b_1$ и матрицы $\mathbf{G_p}$, $\mathbf{G_{m0}}$, $\mathbf{G_{m1}}$ порождают коды.

При выполнении условий леммы 1, из (12) следует, что свободное расстояние $\mathscr{E}(b, c, b_1)$–(Ч)ЕП кодов

$$d_{free} = \min\left\{\hat{d}_1^r,\ \hat{d}_2^r\right\}. \tag{13}$$

Теорема 2. При любой скорости R, $0 < R < 1$ и $b + b1 < c$ существуют $\mathscr{E}(b, c, \nu = b_1)$–(Ч)ЕП коды со свободным расстоянием, удовлетворяющим неравенству

$$\frac{d_{free}}{(n+1)c} = \min_{n=0,1,2,\ldots}\left\{(n+1)\mathscr{H}^{-1}\left(1 - R + \frac{\nu}{(n+1)c}\right)\right\}.$$

Доказательство. Выбор величин b, b_1 удовлетворяет условию леммы 1, следовательно $d_{free} = \min\left\{\hat{d}_1^r,\ \hat{d}_2^r\right\}$. Получим асимптотическое значение для $\hat{d}_1^r$. Минимальное расстояние может соответствовать случаю А.1 или А.2. Рассмотрим случай А.1, когда кодовая последовательность $\mathbf{v}$ состоит из одного блока $\mathbf{v}_t$. Любая кодовая последовательность $\mathbf{v}$ должна удовлетворять условию

$$\begin{bmatrix} \vdots \\ \mathbf{v}_{t-1}^{\mathrm{T}} \\ \mathbf{v}_t^{\mathrm{T}} \\ \mathbf{v}_{t+1}^{\mathrm{T}} \\ \vdots \end{bmatrix}^{\mathrm{T}} \cdot \begin{pmatrix} \ddots & & & & \\ \mathbf{H}_0^{\mathrm{T}} & \mathbf{H}_1^{\mathrm{T}} & & & \\ & \mathbf{H}_0^{\mathrm{T}} & \mathbf{H}_1^{\mathrm{T}} & & \\ & & \mathbf{H}_0^{\mathrm{T}} & \mathbf{H}_1^{\mathrm{T}} & \\ & & & \ddots & \end{pmatrix} = \mathbf{0}.$$

Следовательно, должна выполняться система

$$\begin{cases} \mathbf{v}_t\mathbf{H}_0^{\mathrm{T}} = \mathbf{0}, \\ \mathbf{v}_t\mathbf{H}_1^{\mathrm{T}} = \mathbf{0}. \end{cases}$$

Матрица $\mathbf{H}_0$ имеет $r = c - b$ уравнений, а матрица $\mathbf{H}_0$ – $r_1 = \nu$. Так как элементы матриц $\mathbf{H}_i$, $i = 0, 1$ выбираются случайно равновероятно,

то вероятность случайной последовательности $\mathbf{y}_1$, состоящей из одного блока веса ω, оказаться кодовой равна

$$P\left(\mathbf{y_1}\mathbf{H}^{\mathrm{T}}=0\right)=2^{-r-\nu}.$$

Вероятность того, что минимальный вес одного кодового d_1 блока по ансамблю не превосходит некоторое ω_0 можно рассчитать как

$$P(d_1\le\omega_0) \quad < \quad \sum_{i=1}^{\omega_0}\left(\begin{array}{c} c \\ i \end{array}\right)2^{-r-\nu}<2^{c\left[\mathscr{H}\left(\frac{\omega_0}{c}\right)-(1-R)-\frac{\nu}{c}\right]}. \tag{14}$$

Из неравенства (14) следует, что для любого сколь угодно малого $\varepsilon>0$ эта вероятность стремится к нулю

$$\lim_{c\to\infty}P(d_1\le\omega_0)=0,$$

если относительный вес δ, $\delta=\frac{\omega_0}{c}$ удовлетворяет неравенству

$$\delta<\mathscr{H}^{-1}\left(1-R+\frac{\nu}{c}\right)-\varepsilon. \tag{15}$$

Для кодовой последовательности из двух блоков должна выполняться система

$$\left\{\begin{array}{l} \mathbf{v}_t\mathbf{H}_0^{\mathrm{T}}=\mathbf{0}, \\ \mathbf{v}_t\mathbf{H}_1^{\mathrm{T}}+\mathbf{v}_{t+1}\mathbf{H}_0^{\mathrm{T}}=\mathbf{0}, \\ \mathbf{v}_{t+1}\mathbf{H}_1^{\mathrm{T}}=\mathbf{0}. \end{array}\right.$$

Произвольная последовательность $\mathbf{y_2}$ из двух блоков окажется кодовой с вероятностью

$$P\left(\mathbf{y_2}\mathbf{H}^{\mathrm{T}}=0\right)=2^{-2r-\nu}.$$

Тогда вероятность того, что минимальный вес двух кодовых блоков d_2 по ансамблю не превосходит ω_0 можно рассчитать как

$$P(d_2\le\omega_0) \quad < \quad \sum_{i=1}^{\omega_0}\left(\begin{array}{c} 2c \\ i \end{array}\right)2^{-r-\nu}<2^{2c\left[\mathscr{H}\left(\frac{\omega_0}{2c}\right)-(1-R)-\frac{\nu}{2c}\right]}. \tag{16}$$

Откуда получаем

$$\frac{d_2}{2c}>\mathscr{H}^{-1}\left(1-R+\frac{\nu}{2c}\right)-\varepsilon.$$

Видно, что для кодовых последовательностей с произвольным числом последовательных ненулевых блоков n' выполняется

$$\frac{d_{n'}}{n'c}>\mathscr{H}^{-1}\left(1-R+\frac{\nu}{n'c}\right)-\varepsilon.$$

Так как кодовые последовательности, соответствующие информационным последовательностям из $I_{t,1}$, $I_{t,2}$, могут иметь 1–3 блока, а $n'=\{n,n+1\}$, где n – число соответствующих ненулевых информационных блоков, то

$$\frac{d_{free}}{(n+1)c}=\min_{n=0,1,2}\left\{(n+1)\mathscr{H}^{-1}\left(1-R+\frac{\nu}{(n+1)c}\right)\right\}.$$

□

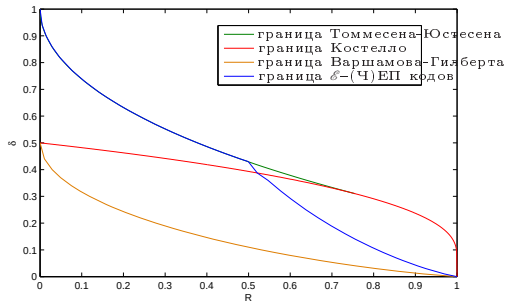

Рис. 1: Асимптотические границы кодов

При скорости $R<0.5$ коды из ансамбля $\mathscr{E}(b,c,\nu)$ обладают полной единичной памятью $\nu=b$. При полной памяти n информационным блокам всегда соответствует последовательность из $n+1$ кодовых блоков. Граница приобретает вид:

$$\delta_{free}=\min_{n=1,2}(n+1)\left(\mathscr{H}^{-1}\left(1-\frac{n}{n+1}R\right)\right)$$

и совпадает с границей ЕП–кодов Томмесена–Юстесена [6]. При скоростях выше $R\ge0.5$ предельная память, удовлетворяющая лемме 1, $\nu=c-b-1$. При максимальной длине кодового ограничения ν граница имеет вид

$$\delta_{free}=\min_{n=0,1,2}(n+1)\left(\mathscr{H}^{-1}\left((1-R)\frac{n+2}{n+1}\right)\right).$$

5. Заключение

Рассмотрен ансамбль двоичных $\mathscr{E}(c,b,\nu)$–(Ч)ЕП кодов, заданный случайными проверочными матрицами (5) с соответствующими порождающими матрицами, удовлетворяющими условию (6). Получена нижняя граница свободного расстояния, совпадающая при $R\le0.5$ с границей Томмесена–Юстесена и уступающая ей и границе Костелло [8] при $R>0.5$. Сравнение с общей границей сверточных кодов (граница Костелло), границей ЕП–кодов и границей блоковых кодов (граница Варшамова–Гилберта)[8] дано на рис. 1.

Список литературы

[1] Lin-Nan Lee. Short unit-memory byte-oriented binary convolutional codes having maximal free distance. *IEEE Transactions on Information Theory*, pages 349–352, May 1976.

[2] Gregory S. Lauer. Some Optimal Partial-Unit Memory Codes. *IEEE Transactions on Information Theory*, 23(2):240–243, March 1979.

[3] V. Zyablov and V. Sidorenko. *On Periodic (Partial) Unit Memory Codes with Maximum Free Distance*, volume 829 of *Lecture Notes in Computer Science*, pages 74–79. 1994.

[4] U. Dettmar and U. Sorger. New optimal partial unit memory codes based on extended BCH codes. *Electronic Letters*, 29(23):2024–2025, 1993.

[5] U. Dettmar and S. Shavgulidze. New Optimal Partial Unit Memory Codes. *Electronic Letters*, 28:1748–1749, August 1992.

[6] Christian Thommesen and Jørn Justesen. Bounds on distances and error exponents of unit memory codes. *IEEE Transactions on Information Theory*, 29(5):637–649, 1983.

[7] G. Forney. Convolutional codes I: Algebraic structure. *Information Theory, IEEE Transactions on*, 16(6):720–738, 1970.

[8] R. Johannesson and K. Zigangirov. *Fundamentals of Convolutional Coding()*. 1999.